УДК 004.9

**Н. А. Вавичкин**
Научный руководитель: д-р тех. наук, проф. В. Л. Кузнецов
Московский государственный технический университет
гражданской авиации, Москва

# МАТЕМАТИЧЕСКИЕ МОДЕЛИ В ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

*Аннотация.* В настоящее время информационные технологии становятся преобладающим направлением научно-технического прогресса. Темпы их развития, а также масштабы внедрения компьютерных техники и технологии приводят к необходимости всеобъемлющей защиты информации. В свою очередь, изучение задачи защиты информации требует построения модели этого явления. Модель может применяться при разработке замысла защиты, в ходе планирования, предотвращения и нейтрализации угроз информационной безопасности. При этом к моделям защиты информации целесообразно предъявлять общие требования, свойственные аналогичным моделям сложных систем.

*Ключевые слова:* информация; безопасность; математическая модель; защита информации.

Не вызывает сомнений тот факт, что информационная безопасность является актуальной проблемой в современном мире. Анализ работы последних форумов по информационной безопасности и активное обсуждение проблем безопасности информации в сети Интернет показал, что наиболее актуальным и перспективным направлением для обеспечения безопасности стало использование математических моделей.

Математическая модель в информационной безопасности — это описание сценариев в виде последовательности действий нарушителей и соответствующих ответных мер. Приближения таких моделей описывают процессы взаимодействия нарушителя с системой защиты и возможные результаты действий [1].

Математическое моделирование для информационной безопасности нашло отражение в фундаментальных исследованиях. В ходе исследований были разработаны:

— математическая модель информационных атак на автоматизированные системы, обеспечивающая возможность представления несанкционированных действий нарушителей в виде графовых структур;

– математическая модель процесса выявления атак, базирующаяся на конечных автоматных распознавателях и позволяющая эффективно выявлять известные и новые типы атак;
– математическая модель процесса оценки рисков безопасности, позволяющая вычислять значение риска с учетом уровня ущерба от атаки, а также вероятности ее реализации [2].

На настоящий момент осуществлена разработка математической модели политики информационной безопасности подсистемы эталонной автоматизированной системы обработки данных на основе эталонной модели защищенной автоматизированной системы [3].

В процессе проектирования сложных систем, таких как комплексные и интегрированные средства защиты информации информационных систем, в большинстве случаев прибегают к моделированию основных процессов, происходящих внутри информационной системы и на стыке «среда — система» [4]. Кроме того, модели могут использоваться для проведения мониторинга и аудита безопасности на этапах эксплуатации и сопровождения систем. Основу моделей обеспечения безопасности информации составляют следующие теории:

– формально-эвристический подход;
– теория вероятностей и случайных процессов;
– эволюционное моделирование;
– теория графов, автоматов и сетей Петри;
– теории игр и конфликтов;
– теория катастроф;
– теория нечетких множеств;
– энтропийный подход.

Отличия большинства моделей заключаются в том, какие параметры они используют в качестве входных, а какие представляют в виде выходных после проведения расчетов. Кроме того, в последнее время широкое распространение получают методы моделирования, основанные на неформальной теории систем: методы структурирования, методы оценивания и методы поиска оптимальных решений [4].

В результате исследования о возможности применения моделирования в информационной безопасности выявлено, что математическая модель должна обладать следующими свойствами:

– масштабируемость;
– наглядность;
– практическая направленность;
– универсальность;
– комплексность;
– простота использования;

– возможность функционирования в условиях высокой неопределенности исходной информации;
– учет различных факторов воздействия на информационные ресурсы.

Как привило, результатами моделирования являются:
– оценка возможности реализации различных угроз на информационные системы и проведения атак на них;
– количественная оценка качества функционирования системы защиты;
– оценка экономической эффективности применения средств защиты информации;
— структура построения системы защиты информационной системы.

**Список литературы**

1. *Щеглов А. Ю.*, *Щеглов К. А.* Математические модели и методы формального проектирования системы защиты информационных систем : учеб. пособие. СПб. : Университет ИТМО, 2015.

2. *Сердюк В. А.* Разработка и исследование математических моделей защиты автоматизированных систем от информационных атак : автореф. дис. ... канд. тех. наук. М., 2004 [Электронный ресурс]. URL: http://diss.seluk.ru/av-informatika/896805-1-razrabotka-issledovanie-matematicheskih-modeley-zaschiti-avtomatizirovannih-sistem-informacionnih-atak.php (дата обращения: 04.11.2017).

3. *Дубровин А. С.*, *Сумин В. И.* Математическая модель политики информационной безопасности подсистемы эталонной автоматизированной системы обработки данных на основе ЭМЗАС-сети // Научные ведомости Белгород. гос. ун-та. 2009. № 1(56). Вып. 9/1. С. 26–44 [Электронный ресурс]. URL: http://dspace.bsu.edu.ru/bitstream/123456789/10304/1/Dubrovin_Matemat.pdf (дата обращения: 07.11.2017).

4. *Курилов Ф. М.* Моделирование систем защиты информации. Приложение теории графов // Технические науки: теория и практика : материалы III Международ. науч. конф. (г. Чита, апрель 2016 г.). Чита : Изд-во «Молодой ученый», 2016. С. 6–9.